AIR WAR COLLEGE

AIR UNIVERSITY

ATTENDED TACTICAL GROUND SENSORS:

A MUST FOR FORCE AND RESOURCE PROTECTION

by

Michael F. Pasquin, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Curriculum Requirements

Advisor: Colonel Ted W. Hashimoto,

Maxwell Air Force Base, Alabama

April 1, 1997

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01APR1997	N/A	-

Title and Subtitle	Contract Number
Attended Tactical Ground Sensors: A Must for Force and Resource Protection	DE-AC22-96EW96405
	Grant Number
	Program Element Number

Author(s)	Project Number
Pasquin, Michael F.	**Task Number**
	Work Unit Number

Performing Organization Name(s) and Address(es)	Performing Organization Report Number
Air War College Maxwell AFB, Al 36112	

Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
The original document contains color images.

Abstract

Subject Terms

Report Classification	Classification of this page
unclassified	unclassified

Classification of Abstract	Limitation of Abstract
unclassified	UU

Number of Pages
52

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Acknowledgment

AU/AWC/RWP-146/97-04

Abstract

Today, force protection is a growing concern of the armed forces. In part, unfortunately, because of the June 25, 1996, Khobar Towers bombing in Saudi Arabia that killed 19 airmen and injured over 400 others. Something must be done *immediately* to better protect our forces and resources as the military is being deployed more and more into places like Saudi Arabia, Rwanda, Somalia, Bosnia, and Haiti. In the future, less is likely to be know about the physical environment where forces will be deployed, and even less, perhaps, will be known about the threat facing these forces. To effectively deal with this future, the military will need the significant advantages obtainable from Attended Tactical Ground Sensor Systems (ATGSS).

The thesis of this paper is that because of the technological advancements in ATGSS, *more* consideration should be given on how to employ them to enhance force and resource protection. This assertion rings true after closely examining what happened at the Khobar Towers, as well as reviewing such things as combined forces exercise reports, key acquisition documents for physical security equipment (PSE), and ongoing PSE research and development activities. The good news is that it is not too late for the military to begin taking advantage of the important contributions of ATGSS.

Before exploring ATGSS applications for military operations other than war, and wartime and law enforcement operations, this paper begins by looking at what ATGSS are available to the military today. Only marginally sufficient to aid in force protection,

current ATGSS are in serious need of upgrade or replacement. Next, the ATGSS technological advancements being pursued will be highlighted. These advancements are astonishing in many regards and could standardize the way future security is provided.

Chapter 1

Introduction

The U.S. military was *not* prepared for the bomb that killed nineteen airman and injured over 400 others at the Khobar Towers at Dhahran Air Base in Saudi Arabia. Attended Tactical Ground Sensor Systems (ATGSS) could have made the difference, yet, they received little consideration before the bombing. (ATGSS are defined as small, lightweight sensors that can normally be carried by military police (military police in this paper refers to Air Force security police and Army and Marine military police) during field conditions for detecting intruders entering a secured area. Forces in the immediate vicinity monitor sensor alarms. In contrast, unattended tactical ground sensor systems (UTGSS) are designed primarily for the military intelligence community to detect and classify such things as wheeled and tracked vehicles. UTGSS can report alarms over great distances, even using satellites, and human operators are normally not present.[1])

The thesis of this paper is that because of the technological advancements in ATGSS, *more* consideration should be given on how to employ them to greatly enhance force and resource protection during future military operations. These operations are thrusting the military more and more into environments like Rwanda, Somalia, Haiti, and Bosnia,—military operations other than war (MOOTW) where very little will likely be known

about the physical environment beforehand. Even less, perhaps, will be known about the threat that forces will confront.

While ATGSS were given little thought in Saudi Arabia, this paper will also show that there is insufficient consideration for how these sensors might contribute to force and resource protection during wartime operations. This becomes apparent when examining combined forces exercise reports, the preparation of important documents related to ATGSS acquisition, and ongoing physical security equipment research and development.

The paper concludes with a brief look at the possibilities that ATGSS can offer to law enforcement as well; if considering ATGSS for this arena begins today.

To lay a foundation for discussing ATGSS, opening chapters will present a basic summary of the ATGSS currently fielded today. Although these systems are still somewhat effective, they employ technology that is decades old and in dire need of replacement. An overview follows of the basic research and development underway by the Air Force and the Army to improve or replace these outdated systems. The Navy is not discussed because it uses ATGSS developed by either the Air Force or the Army.

Notes

[1] The Joint Staff, background paper, subject: Unattended MASINT Sensors, 10 September 1996, 1.

Chapter 2

Currently Fielded ATGSS

The following is a description of currently fielded ATGSS. The list is very short. Two out of the three systems are virtually antiques that will appear even more outdated when considering the next chapter's discussion of the technological strides being made in ATGSS technology.

Miniature Intrusion Detection Systems (MIDS)

MIDS is a small, lightweight sensor system based on Vietnam-era technology. A basic package weighs 23 pounds and consists of five sensors (a combination of breakwire, breakbeam (active pulsed infrared) and seismic), one radio transmitter for each sensor to transmit alarms, and a hand-held monitor. Each sensor has a range of approximately one to 30 meters, except for the breakwire sensor's wire that can be strung out up to 250 meters.[1]

Some limitations of MIDS are that the sensors can only transmit alarms to the hand-held monitor on one frequency. This can be a problem in the many countries like Korea where frequency allocations may be limited. Also, MIDS only has a hand-held, battery operated monitor to receive alarms—unlike TASS (discussed below) that has a laptop and a desktop annunciator. Finally, the system does not meet the Army's operational

temperature requirements for tactical sensors of minus 40 degrees Fahrenheit to plus 140 degrees Fahrenheit.[2]   Figure 1 is a drawing of the MIDS breakbeam sensor.
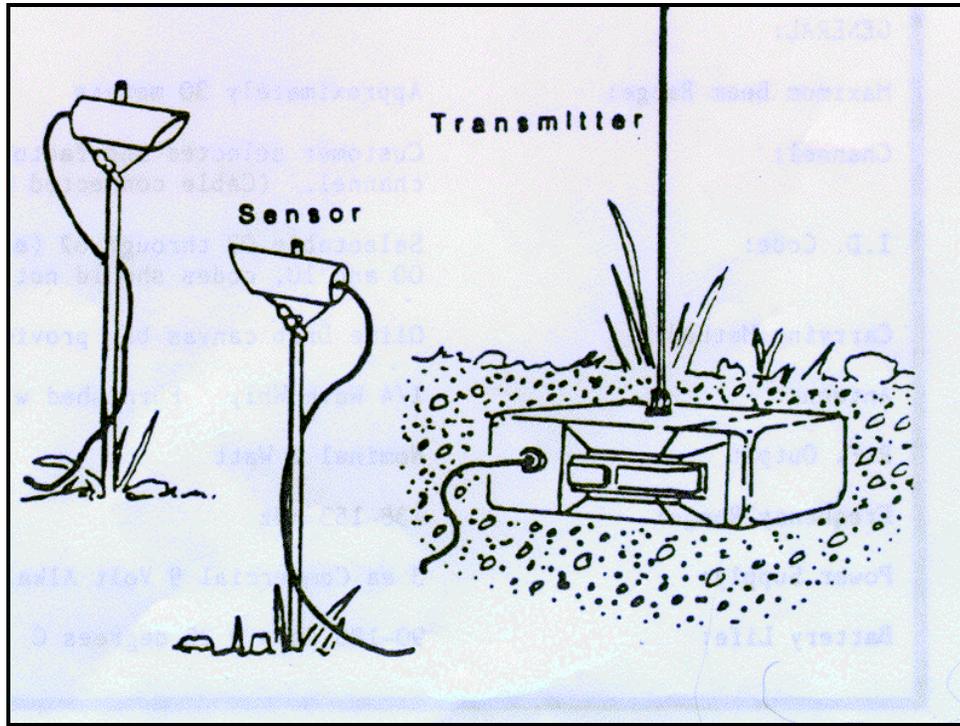
Source: From Qual-Tron Incorporated, information paper, subject: Miniature Intrusion Detection System (MIDS), undated: 4)

Figure 1. MIDS Breakbeam Sensor

In figure 1, the sensor transmits a beam to a receiving sensor. Breaking the beam generates an alarm. The transmitter sends an alarm message via radio frequency to a hand-held monitor.

Platoon Early Warning System (PEWS)

PEWS is an Army AGTSS that is similar to MIDS in that it consists of small, lightweight components based on decades-old technology. A basic package consists of ten sensors that detect ground vibrations from intruders or magnetic signals from

vehicles, two radio receivers, two interface wire links, and other accessories packaged in two carrying bags that weigh 11 pounds.[3]

PEWS sensors have considerable limitations. They annunciate alarms on only one frequency, lose considerable effectiveness in loose soil, have a probability of detection that is only around 70% in bad weather, and are time consuming to emplace.[4] Also, similar to MIDS, PEWS does not meet the Army's operational temperature requirements and there is only a hand-held monitor for receiving alarms.

Improved Remotely Monitored Battlefield Sensor System (IREMBASS)

IREMBASS consists of sensors designed to be either an ATGSS or an UTGSS—the latter because it detects and classifies moving personnel and wheeled and tracked vehicles. A basic IREMBASS package weighs 25.25 pounds and consists of three sensors (seismic or acoustic, infrared, and magnetic), a monitor display and a radio repeater.[5]

Some system limitations are the sensors' considerable weight (each one is between 4.49 and 5.25 pounds) and its inability, similar to MIDS and PEWS, to meet Army operating temperature requirements.[6]

Notes

[1] Qual-Tron Incorporated, information paper, subject: Miniature Intrusion Detection System (MIDS), undated, 2.

[2] Army Physical Security Equipment Management Office, sensor matrix, subject: Tactical Sensor Comparison Matrix, undated, 5.

[3] Army Communications and Electronics Command, sensor descriptions, subject: Technical Information on the Platoon Early Warning System, 9 September 1996, 1.

[4] Michael Johnston, Computer Science Corporation, telephone interview, 13 September 1996.

Notes

[5] Army Material Systems Analysis Activity (AMSAA), background paper, subject: AMSAA Independent Evaluation for IREMBASS Production Decision, 13 May 1992, 1.
[6] Army Physical Security Equipment Management Office, sensor matrix, 1.

Chapter 3

ATGSS Technological Advancements

Both the Air Force and the Army are performing research and development on ATGSS. There is, fortunately, continuous coordination between these services to eliminate as much duplication of effort as possible. The Air Force is tasked by the Department of Defense Directive (DOD) 3224.3 ("Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support"), to do for exterior PSE what the directive's title spells out, while the Army is tasked with the same responsibilities for interior PSE.[1] Exterior PSE includes sensors like ATGSS that are outdoor sensors designed to detect intrusions at or external to an installation's perimeter. Interior PSE, on the other hand, includes sensors used to detect intrusions inside an installation's perimeter such as balanced magnetic switches used on doors, or volumetric sensors used inside buildings.

Despite the guidance in DOD directive 3224.3, the Army is still involved in developing exterior PSE because technological advancements are blurring the distinctions between exterior and interior sensors. The directive is being rewritten and will include new PSE terminology and different research and development responsibilities.

The following discusses exterior PSE (ATGSS) being developed by the Air Force and the Army.

Air Force

Tactical Automated Security System (TASS)

TASS is evidence that the military services are demanding ATGSS that are more lightweight, durable, and operationally flexible than ever before. TASS was very recently developed for wartime and MOOTW. Its primary use is for securing an installation's perimeter, or protecting high-value assets such as aircraft on a flightline or mobility equipment. TASS consists of a variety of the MIDS sensors discussed above (breakbeam, breakwire, and seismic) with one important difference—a new, sophisticated communications module (transmitter) that gives each sensor a capability to broadcast alarms on up to 8000 selectable radio frequencies.[2] This means that there are few, if any, limitations in countries that might authorize only a limited number of radio frequencies for broadcasting alarms. To receive and display alarms, TASS has a hand-held monitor that displays multiple alarms simultaneously, a graphics-based laptop annunciator, and a desktop annunciator that allows the importing of maps from several sources like CD-ROMs or a scanner.[3] All these components, except for the desktop annunciator, are powered by disposable or rechargeable batteries, or solar panels.

Also part of TASS are thermal imagers that act as assessment devices during day or night, as well as in inclement weather. There are hand-held or weapon-mounted ones, and remotely monitored (through a cable connection) wide-area surveillance ones. The latter can be placed on a tripod a few feet off the ground or mounted just about anywhere,

like the top of a building. Both types of thermal imagers can detect a man-sized target as far as 2.5 kilometers away.[4]

The final element of TASS, designed for the protection of high-value or priority resources, is the tripod mounted monostatic (a single transmitter dish) microwave sensor. With a range of approximately 100 meters, it can be set up so that the fields of coverage overlap for better detection.[5] A bistatic microwave sensor that has two dishes, one to transmit a beam and one to receive it, has a range of approximately 300 meters. It is being studied and may be part of TASS as well.

TASS' operational testing was completed over the summer of 1996. Air Force security police should start receiving approximately $47 million of TASS deliveries later in 1997 and over $100 million in deliveries spread between 1998 and 2003.[6] Other services' military police will also be buying TASS very soon, although specific dollar amounts and delivery timing are undetermined.

Advanced Exterior Sensor (AES)

AES is currently undergoing exploratory development with the Defense Special Weapons Agency (DSWA—formerly the Defense Nuclear Agency). AES transitions to the Air Force in early 1997 and will undergo approximately three to four years of further development before being fielded. It is truly revolutionary in that it is an "area" sensor and not a "point" sensor like the majority of ATGSS discussed in this paper. With a "point" sensor, a beam of energy or a wire has to be broken to generate an alarm. AES is an "area" sensor because it scans for intrusions over a wide area. This is done by means of a cylindrical-shaped sensor unit called a remote sensor monitor (RSM) that is approximately 15 inches in diameter by 30 inches high. The RSM contains three separate

sensors (Fig 2 is an AES RSM) that consist of a low-power radar (millimeter wave), an infrared linear scanning array, and a visible linear scanning array (video motion detector).[7] All three sensors, rotating on a platform 360 degrees each second, annunciate alarms on a display control module (DCM) that is similar to a computer monitor. The DCM will acquire and process alarms from up to 16 RSMs.[8]
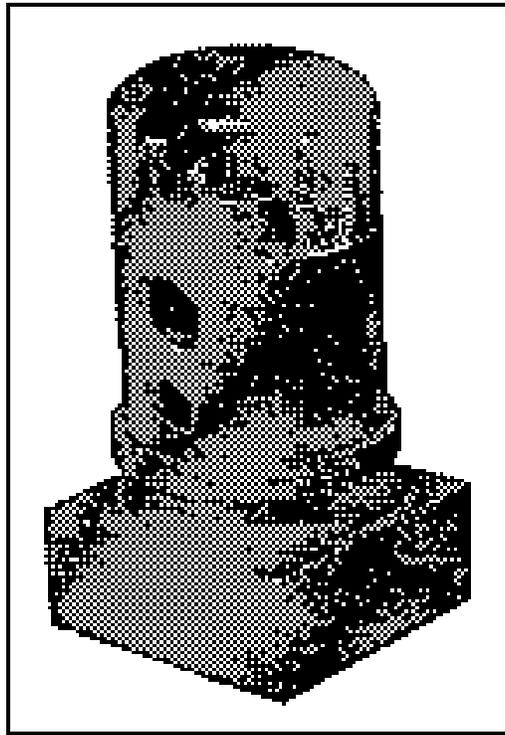
Source: From Sandia National Laboratory, information paper, subject: Advanced Exterior Sensor, May 1994: 1)

Figure 2. AES RSM

Under good or clear weather, the RSM's sensors can detect people walking at 500 meters away or crawling at 250 meters away, and moving vehicles at 1000 meters away.[9] These ranges are not significantly reduced even under a "variety of environmental conditions ranging from day or night, hot or cold, dry to humid and rainy or snowy."[10]

Similar to TASS, AES is being designed to be portable for rapid deployments. In a typical coverage pattern, RSMs can be set up to overlap coverage with other RSMs,

covering up to a "one kilometer area with a wide enough field of view for uneven terrain. Areas of routine activity can be masked out by azimuth and elevation location and/or range to allow high-confidence in all other areas."[11] Masking out areas is a particularly good feature that none of the currently fielded ATGSS have. (The next chapter provides additional details on AES, including deployment scheme diagrams.)

Passive Millimeter Wave Sensor (PMMWS)

A current limitation of ATGSS is that they detect intruders through such measures as infrared-based or microwave-based technology that requires line-of-sight access to an intruder. A need was identified several years ago for a sensor that detects through such obstacles as foliage and other substances described in the next paragraph. DSWA is working with the Air Force and the Applied Research Laboratory at the University of Texas to develop PMMWS to see through such obstacles.[12] The project is currently in the exploratory development phase and will be part of a TASS pre-planned product improvement in the next three to five years.

PMMWS will detect the thermally emitted radiation from a target in the millimeter part of the electromagnetic spectrum.[13] "Millimeter wave lengths are longer than those emitted by passive infrared sensors and can penetrate non-metallic substances with low moisture content. These substances include most types of clothing, most plastics, and commonly used construction materials, such as sheet rock and plywood."[14] Most importantly from a security standpoint, testing is underway to see if the sensor can be adapted to see through foliage.[15] Additionally, PMMWS have one big advantage over other sensors. They will be able to detect an outdoor target such as a human being up to 200 feet away with a temperature of 98.6 degrees Fahrenheit, even with an ambient air

temperature of 99 degrees Fahrenheit and even in fog, mist, and other atmospheric obscurants.[16] These are conditions when, for all practical purposes, infrared sensors are blind.

Millimeter Wave Data Link (MMWDL)

Future tactical ground sensors will require a robust, secure communications medium to transmit alarms that will counter hostile jamming or interference attempts. To meet this challenge, DSWA is developing a MMWDL. Besides being nearly jam resistant, it is a focused beam, whereas UHF and VHF radio transmissions are omnidirectional. The MMWDL can carry large amounts of data that can transmit video images as well as sensor alarms.[17] And because the link is millimeter-wave based, it is minimally interfered with by poor weather such as fog, snow, or heavy rain. It also offers a much greater availability of frequencies compared to the VHF or UHF bands.[18] (While the MMWDL is not an ATGSS, it is mentioned here because of its significance in greatly enhancing future ATGSS alarm transmission security.)

Army

Platoon Early Warning Device II (PEWD II)

The Army has a PEWD II operational requirements document (ORD).[19] (An ORD is a "formatted statement containing performance (operational effectiveness and suitability) and related operational parameters for a proposed concept or system."[20]) PEWD II is being looked at to replace PEWS. It is still in the conceptual stage until coordination is complete between the Army and Air Force to see how many of the PEWD II requirements can be met by TASS.

Similar to TASS, the PEWD II requirement is for a simple, compact, and lightweight AGTSS consisting of a carrying case, hand-held monitor, and a mix of sensor types, eg., seismic, acoustic, magnetic, and infrared. A package consisting of one hand-held monitor, five sensors and the carrying case should not exceed 13 pounds.[21] PEWD II will be capable of "detecting intrusions into protected areas, and rapidly communicating detection, direction, classification and assessment alarm messages, both visual and aural, through the monitor to an operator."[22]

An important consideration is that PEWD II must be rugged enough to withstand the vigorous handling and stress encountered in combat. This means it must not be affected by an airdrop if it is in an airborne soldier's rucksack, or by the vibrations from being transported in combat vehicles.[23]

Multipurpose Security and Surveillance Mission Platform (MSSMP)

MSSMP, similar to the Air Force's AES program, could also represent a significant leap in the ATGSS' capabilities. As seen in figure 3, MSSMP is a flying, doughnut-shaped platform. It is based on a ducted-fan, vertical-take-off-and-landing air vehicle approximately six feet in diameter, 30 inches high, and capable of traveling up to 10 kilometers from the base station.[24] For the prototype unit, the operator's control display station is a laptop computer running a graphical Windows program.[25]
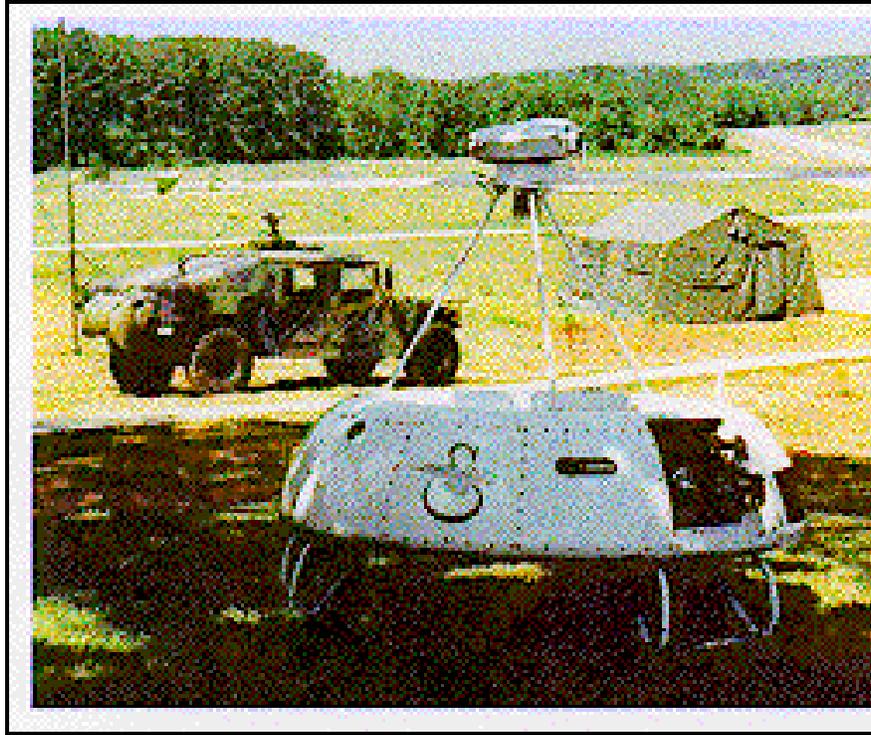
Figure 3. MSSMP

MSSMP carries a small sensor suite that consists of three commercial-off-the-shelf sensors, a visible light video camera for video motion detection, an infrared video camera, and a laser range finder.[26] This suite, mounted on a pan-and-tilt zoom unit, weighs approximately 30 pounds.

Family of Integrated Tactical Security Systems (FITSS)

FITSS is a new concept driven by Army requirements under Force XXI to provide current and futuristic security technology for both point and area security.[27] It is intended for all major security missions through the full spectrums of wartime and MOOTW. According to a concept statement for FITSS:

FITSS will address all the diverse aspects of area security (e.g., area reconnaissance, rear operations, security of designated personnel, and equipment) and that of point security (e.g., facilities, command posts and critical points). Since it will be a family of interoperable security systems based on common technologies and configured to meet mission requirements, it can easily be tailored to perform numerous missions even though the missions are dissimilar in nature.[28]

Similar to PEWS II, this project is still in the conceptual stage.

Notes

[1] DOD Directive 3224.3, Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, and Evaluation, Production, Procurement, Deployment, and Support, 17 February 1989, 6.

[2] Wayne K. Messner, "Air Force Systems Mold Defense Asset Security," *National Defense*, February *1995*, 32.

[3] Wayne K. Messner, "Organization is Key to Air Force Security System," *Access Control*, April 1995, 2.

[4] Air Force Electronic Security and Communications Center of Excellence, brochure, subject: Tactical Automated Security System (TASS), 20 October 1994, 4.

[5] Ibid., 3.

[6] John Mitchell, Lt Col, Headquarters U.S. Air Force security police staff, email, 1 January, 1997.

[7] Sandia National Laboratory, briefings slides, subject: Advanced Exterior Sensor Program Review, 16 April 1996, 3.

[8] Ibid., 8.

[9] Scott A. Nicholas and R. Brian Naylor, information paper, subject: Reliable Motion Detection of Small Targets in Video with Low Signal-to-Clutter Ratios, undated, 2.

[10] Daniel A. Pritchard, information paper, subject: System Overview and Applications of a Panoramic Imaging Perimeter Sensor, undated, 281.

[11] Sandia National Laboratory, information paper, subject: Advanced Exterior Sensor, May 1994, 1.

[12] Michael F. Pasquin, transition plan, subject: Defense Nuclear Agency Physical Security Equipment (PSE) Exploratory Development to Advanced Development Transition Plan for Passive Millimeter Wave Sensor—Exterior (PMW-E), 22 May 1995, 1.

[13] Robert L. Rogers, draft final technical report, subject: Passive Millimeter Wave Sensor, 4 October 1996, 14.

[14] Ibid., 15.

[15] Robert L. Rogers, Applied Research Laboratory, University of Texas, email, 2 February, 1997.

[16] Ibid., 16.

[17] Robert L. Rogers, Applied Research Laboratory, University of Texas, email, 12 December 12, 1996.

Notes

[18] Pasquin, Transition Plan for PMW-E, 1.

[19] Army Infantry Center, operational requirements document, subject: Draft Operational Requirements Document for the Platoon Early Warning Device II, 7 March 1996.

[20] DOD Directive 5000.2-M, *Defense Acquisition Management Documentation and Report*, February 1991, 2-1.

[21] Army Infantry Center, operational requirements document, subject: Draft Operational Requirements Document for the Platoon Early Warning Device II, 7 March 1996, 2.

[22] Ibid.

[23] Ibid.

[24] Army Physical Security Equipment Management Office, information paper, subject: Multipurpose Security and Surveillance Mission Platform, undated, 2.

[25] Ibid.

[26] Ibid.

[27] Army Training and Doctrine Command, draft concept, subject: Concept Statement (Final Draft) Family of Integrated Tactical Security Systems, undated, 1.

[28] Ibid., 3-4.

Chapter 4

Considering ATGSS

With the above information providing a background on fielded ATGSS and related research and development efforts, it is now appropriate to discuss the criticality of the military giving more consideration to employing ATGSS. The MOOTW environment is discussed first because of its immediate impact on military forces today. An examination follows on the lack of regard given ATGSS in the wartime environment. Finally, there will be a brief look at ATGSS and the law enforcement arena. The main focus will be on nearly-fielded systems like TASS, or ones that are under development like AES or MSSMP. Although other ATGSS like FITTS or PEWD II are supported by proper acquisition documents like a mission need statement (MNS) and an ORD, they are still in the conceptual stage and may or may not be developed further. (A MNS is a document no more than five pages in length that identifies a non-system-specific mission area need or deficiency.[1])

Military Operations Other Than War (MOOTW)

MOOTW that could involve the military include "humanitarian missions (feeding, protecting, and relocating refugees; disaster relief; and assistance in civil disorders), counterdrug operations, noncombatant evacuation, peacekeeping and hostage rescue

operations."[2] A recent MOOTW environment for U.S. forces was at the Khobar Towers. The June 25, 1996, bombing there is discussed first, followed by a brief look at ATGSS' role in future MOOTW environments involving nonlethal weapons.

The bombing of the Khobar Towers provides, regrettably, the ultimate stimulus to propel the military to study much more thoroughly the uses of ATGSS. In the future, U.S. forces will invariably be involved in similar missions as the national strategy of enlargement and engagement has "committed the United States to the security of friends and allies throughout the world."[3] Therefore, as U.S. forces will be maintaining a physical presence or deploying overseas on short notice to demonstrate this commitment, ATGSS must be factored in.

The bombing was investigated by retired General Wayne Downing, the former Commander-in-Chief of U.S. Special Operations Command. Results of the investigation were documented in "The Downing Report" that reveals the inadequacy of the security provided for the Khobar Towers, as well as what levels of priority physical security had received for funding throughout the U.S. Central Command's area of responsibility, the responsible command for this region of the world. The following examines the overall security conditions prevailing at the time of the bombing as a framework for discussing the conclusion that there was little thought given to employing or funding technology. This is technology that relates directly to ATGSS.

The Khobar Towers represents perhaps one of the most difficult security challenges the military can face apart from a wartime environment. Living quarters there were primarily high-rise apartments up to eight stories tall. The complex also included office space and administrative facilities. The perimeter of the U.S., French, and British area

was surrounded by a fence and a row of concrete Jersey barriers. Buildings 131 and 133, the ones most severely damaged during the bombing, are eight-story apartment complexes facing the north perimeter.[4] There is a parking lot outside this north perimeter that is next to a group of houses. From the perimeter fence outward near the Khobar Towers was the responsibility of Saudi Arabian forces, while security inside the fence was the responsibility of U.S. forces.

It is also important to note the circumstances surrounding the threat conditions before the bombing. (Threat conditions are assigned on a variable scale from Alpha through Delta: Alpha referring to a minimal threat from terrorism, Bravo and Charlie referring to a more serious threat, and Delta meaning there is a significant threat.) In April of 1996, as the terrorist threat escalated, the Air Force's 4404th Support Group Commander discussed the possibility of raising the threat condition from Bravo to Charlie—a change that would have required the use of additional personnel.[5] The Downing Report states that there was a decision not to go to threat condition Charlie that "appeared to have been based on the availability of security forces and their ability to sustain operations for an extended period of time, rather than what was required by the threat."[6]

Considering the above circumstances, what thought was given to technology prior to the bombing? According to the Downing Report:

> Technology was not widely used to detect, delay, mitigate, and respond to acts of terrorism. Modern equipment for force protection and physical security was either not available or not widely used in the theater. U.S. Army Forces Central Command locations within the theater had minimal access to such equipment. U.S. Naval Forces Central Command used rudimentary technology for perimeter security. Headquarters, U.S. Central command had only a limited ability to provide advice and training to deployed forces on force protection systems.[7]

While it is not the intent of this paper to condemn or criticize military action or inaction in providing effective force protection, ATGSS must be considered *now* for locations like Saudi Arabia where such systems can be especially useful in enabling the military to compensate for such challenges as manning deficiencies and the need to provide better perimeter protection. For example, any thermal imager can offer several important advantages for deployment locations like the Khobar Towers. Such thermal imagers can be used to provide 24-hour coverage well beyond any fence line. If the threat is high enough, as it would be under threat condition Charlie or Delta, military police would not have to be posted to observe vulnerable areas along a perimeter, or anywhere else for that matter. Air Force security police at the Khobar Towers "were on 12-hour shifts for six days or longer. Some worked on the same observation post for 12 hours at a time exposed to 100 degree heat, with only meal and comfort breaks."[8] Under these conditions, it could have been security police using remotely monitored thermal imagers during the day of the attack that spotted the truck carrying the bomb—not the exhausted security police posted on top of one of the buildings.

Thermal imagers should be appreciated even more as the quintessential ATGSS in light of the follow-on actions resulting from the Downing Report to correct identified security deficiencies. Secretary of Defense William J. Perry announced in a September 16, 1996, report to the President that:

> First, with the full cooperation and support of the Saudi Arabian government, we will begin immediately to relocate our deployed air forces (4404th Air Wing) from Saudi air bases located in urban concentrations at Riyadh and Dhahran to an isolated location at the uncompleted Prince Sultan Air Base near Al Kharj, where many coalition forces were located during the Gulf War. While our personnel will be living in tents initially,

we will be able to construct very effective defenses against terrorist attacks.[9]

In a related statement, Senator John Glenn said in the July 22, 1996, edition of the Air Force Times: "In the desert, U.S. troops could establish mile-wide perimeters if they want to."[10] In this new environment, the easiest way to observe vast perimeters, and the least demanding for military police, would be to use wide-area thermal imagers mounted as high off the ground as possible.

Other elements of ATGSS can be used in an urban-type environment to help preserve the integrity of any stand-off distance around a perimeter. This can be accomplished with TASS' sensors, or even currently fielded sensors like the old MIDS. Once the stand-off area is established by such things as ropes or Jersey barriers, sensors could provide a virtual guarantee of detecting threats like cars or trucks approaching the perimeter. While sensors cannot prevent people or vehicles from approaching, military police will at least be notified that the stand-off distance was compromised.[11]

For receiving ATGSS alarms, TASS or IREMBASS offer a hand-held monitor (TASS offers a laptop annunciator as well) that will receive alarms generated by multi-frequency capable sensors. Roving security patrols in vehicles, or individuals on foot patrol, can have hand-held or laptop monitors to receive alarms on one frequency so all military police will know where an alarm originates from. Alternatively, individual frequencies can be allocated to the various sections of a base or area. This way, each sector's assigned military police would only receive alarms for their particular sector.

Future force protection in the MOOTW environment will require more consideration to the interplay between ATGSS and nonlethal weapons. In Mogadishu, in March 1995,

military police were tasked to help United Nations' troops withdraw. During this operation, Marines were armed with nonlethal technology that included stick and aqueous foam guns, pepper spray, rubber bullets, wooden shotgun pellets, bean bags (fired from shotguns), and stinger grenades with rubber pellets.[12] Because of the unique capabilities nonlethal weapons offer, military police are being urged to exploit the development and use of these weapons and to adapt them to military police operations.[13]

ATGSS' role in the nonlethal MOOTW environment, not explained in any ATGSS concept of operations (CONOPS), has to include one of the greatest benefits these systems have to offer—the element of time. (A CONOPS is a written document that goes beyond the operational descriptions mentioned in an ORD. For example, it would discuss in considerable detail things like the physical terrain where a particular ATGSS would be employed depending on the size of the area to secure, the current threat condition, and the number of available military police.) By properly employing such ATGSS like thermal imagers for around-the-clock surveillance, and any ATGSS sensors like TASS offers, time is acquired. Time offers the added flexibility, often not needed in a lethal environment, to assess any situation and decide what spectrum of force is necessary— from nonlethal to lethal. Also, as will be seen next for the wartime environment, ATGSS should free up more forces from the detection mode, allowing them to respond quicker to any given situation.

Along with planning ATGSS for the above near-term MOOTW applications, multi-service consideration should also be given to future ATGSS like AES and MSSMP. AES' video motion detection capability will eliminate the requirement to monitor assessment equipment full-time. Additionally, AES' three separate sensors will greatly

increase the odds of detecting intruders under any weather condition, day or night. Unfortunately, the discussion below reveals that considering AES for force and resource protection has been lacking.

MSSMP, although much further away from being fielded, should be especially useful for counterdrug missions and border patrol operations where surveillance is required of areas at a considerable distance (up to ten kilometers) from a base station. Essential to this system is that its employment schemes also be incorporated in well thought out multi-service CONOPS. Considering MSSMP now will allow ideas adequate time to mature by the time the system is employed.

Wartime Operations

For discussion purposes, this section focuses on air base security because it is a joint Air Force and Army operation, and because it provides an excellent example of a critical wartime tasking. In securing an air base, the Air Force security police provide security inside the perimeter, while the Army military police provide security outside the perimeter.[14] Based on the formidable capabilities and potential of the Air Force weapon systems, future adversaries "may feel strongly inclined toward neutralizing or, at a minimum, blunting U.S. airpower. Such opponents have a menu of options available, among the potentially most effective being to attack Air Force bases."[15] And why not attack an air base? "The Air Force's growing reliance on fewer, more vulnerable aircraft, such as AWACS, JSTARS, and Rivet Joint aircraft, makes airpower in some ways more vulnerable now than during the Cold War. All these special assets are too large to park in hardened hangars, yet too delicate to be safe on an airfield."[16] (AWACS is the Airborne

Warning and Control System aircraft and JSTARS is the Joint Surveillance and Targeting System aircraft.)

A brief look at history shows how air bases, or any site or installation for that matter, might be attacked in the future to highlight the importance of properly defending them with ATGSS. Out of 645 attacks on air bases from 1940 to 1992, 83% of attackers used foot travel at some point—and in a majority of the attacks, the operation was entirely unmotorized.[17]   Most important to consider is that 75 percent of these attacks were standoff in nature where weapons like mortars, surface to air missiles, or large caliber sniper rifles were used that can be employed up to several kilometers from the base's perimeter; as compared to penetrating attacks that were 22 percent (where the hostile forces actually penetrated the base as they often did during World War II); or combined attacks (standoff and penetrating together) that were only three percent.[18]

With this historical perspective in mind, of all the ATGSS discussed above, TASS appears to be the most promising for base defense as it offers an effective assessment and detection capability in one package. And unlike other ATGSS still being developed, TASS will be available initially to the Air Force later in 1997 and the other services soon thereafter. Regrettably, as close as this system is to fielding, the following look at exercise Foal Eagle shows that thinking ahead and formally planning how TASS can best be used for force and resource protection has been inadequate.

Foal Eagle is a rear area, combined, force-on-force exercise hosted annually by the Air Force in South Korea. As part of Foal Eagle 1993 and 1994, held at Osan and Kunsan Air Bases respectively, evaluation of pre-production TASS equipment provided valuable insights that were either overlooked or never given proper prior consideration.

24

Positively speaking, before looking at these insights, it is worth noting that Foal Eagle did demonstrate how effective TASS could be in detecting the attacking opposing force (OPFOR). At Osan, for example, the TASS thermal imager operator effectively directed a counter attack against the OPFOR despite the OPFOR completely masking their movement with…smoke.[19] (The thermal imager was several feet off the ground mounted on a tripod.) Also at Osan, numerous TASS sensors covered likely OPFOR approach avenues along the base's perimeter. These sensors were effective in friendly forces being able to neutralizing roughly 30 percent of the OPFOR attacks.[20] A significant finding was that when more than one layer or line of sensors was employed, the path or direction of the intruders could be discerned. With a single line of sensors, alarms would only indicate the location of an intrusion.

Also of positive note, at Kunsan, an idea evolved to mount two thermal imagers as high up in the air as possible. One was placed on top of the base water tower on the contonment side of the base (175 feet high), and one was placed on top of an old security observation tower (70 feet high) on the opposite side of the base near the flightline.[21] Between both thermal imagers, nearly every approach to the base was covered except for a few places that were on the back side of hills. Amazingly, the OPFOR was detected approaching the base from at least one kilometer away, well before the base perimeter was penetrated, as it was sometimes done at Osan. In fact, after the exercise was concluded, it was learned that the OPFOR referred to the outside perimeter near the contonment area as the "killing fields" since their forces were defeated there so often by Air Force security police being directed by thermal imager operators.[22] TASS' sensors were employed similar to how they were at Osan, along likely OPFOR approach avenues

that turned out to be selected points along the sea coast and next to the base water tower. At these locations, steep hills and rock formations precluded observation by either of the thermal imagers.

Unfortunately, Foal Eagle's negative aspects speaks to the overall lack of consideration given to TASS. While utilizing the thermal imagers and tactical sensors as noted at Osan and Kunsan air bases was indeed effective, further examination of exercise reports revealed that at Kunsan, as well as at Osan, "no written procedures were available to help the defense forces employ the sensor systems. This situation was made worse by not having a sufficiently detailed CONOPS that would have shown how the systems should be employed."[23] Without such documentation, military police in the future are left with no choice but to use "trial and error" methods—unacceptable in wartime where time may be extremely limited. The sensors worked well at Osan and Kunsan, in large part, because they were set up by the security police and engineers assigned to the Air Force program office responsible for developing TASS.

This situation speaks to the injustice done by not embracing all the possible aspects technology has to offer. Millions of dollars are going into developing TASS, and enough has been learned about ATGSS over the last several years that a detailed TASS CONOPS should have been written long ago. An attempt was made by the Air Force's Air Combat Command security police staff in 1994 to develop such a document. Unfortunately, it was very short and did little more than briefly describe each TASS sensor and offer a few sentences on how they might be employed.[24] It also only addressed Air Force needs, which leads to another conclusion that any ATGSS CONOPS should be joint so as to address all the services' specific requirements.

26

In this CONOPS, the Marine Corps military police, for example, might have similar wartime requirements to secure a contonment area. For such an area, along with TASS' sensors, its tripod-mounted monostatic microwave sensors would be as useful for securing fuel depots or areas where there was high pilferage, as they would be for securing aircraft on a flightline.   Yet no formal consideration has been given to microwave sensors being used for any other purpose but aircraft protection.

While the above discusses fielded or soon to be fielded ATGSS, it is not too early to be thinking about the employment of future sensors such as AES.   Regrettably, consideration for this triple-sensor system has also been lacking. This should not be acceptable for a system that has had over $2 million spent on it from its inception through 1996, and has an additional $5.7 million budgeted over the next several years to complete its development.[25]   In reality, there is even more money than this involved. There were two other PSE projects similar to AES that several million dollars were spent on. These projects were eliminated several years ago for complex reasons relating to computer capabilities. Fortunately, their technology base was able to be transferred to the AES program.

Although AES is currently undergoing applied research, with expected fielding probably in the next five years, there is no service-wide or even Air Force-only wartime oriented employment theory or CONOPS. From a service-wide perspective, an office under the Secretary of Defense chairs a Physical Security Equipment Action Group (PSEAG) meeting that brings all the service PSE managers together on a quarterly basis. While services are aware of AES through such meetings, there has been no impetus to develop a joint employment scheme in coordination with Sandia National Lab (SNL) who

is performing the applied research on the project, and the Air Force Material Command's Electronic Security and Communications Center of Excellence (ESC/AVJ) who will complete the development work and field the system.

From the Air Force-only side, Air Force Space Command (Space Command) has had a MNS for several years, and the command is working on an ORD for a Wide-Area Security System (WASS) to clear and monitor space launch complexes. The MNS states that:

> DOD space policy requires the assured access to space and security measures commensurate with the threat and intended use of the system during peace and international conflict. Both East and West launch sites require an operational, cost effective system which is able to detect and assess the presence of unauthorized personnel within the launch operations area/safety hazard zone during periods critical to spacecraft orbital insertion.[26]

Space Command would like to see AES satisfy their need for a WASS. Unfortunately, the MNS notwithstanding, the WASS' desperately needed ORD is long overdue and is needed to link WASS to AES. This is not a good situation since SNL has been developing AES primarily to fulfill WASS requirements. Furthermore, just as there is no joint AES CONOPS, there is no Air Force AES CONOPS covering how other major commands would like to see AES employed in a wartime environment to do such things as, for example, integrate technologically with TASS.

Also worth mentioning from an Air Force-only standpoint, security police at the Air Staff have developed a Priority Resource Security System ORD that has a generic requirement for an area-based ATGSS that could be met with AES.[27] However, this ORD is at best only a starting point for developing a CONOPS.

While AES will be too large to deploy at a great distance from an installation as other ATGSS are, an employment scheme should be considered requiring, whenever possible, a detailed terrain analysis of locations where forces might be employed. If such an analysis is not possible, some type of generic employment as figure 4 depicts would do for a small area where valuable resources are located. In this figure, two RSMs are deployed to capitalize on the ability to overlap coverage and protect a site up to 300 meters across.
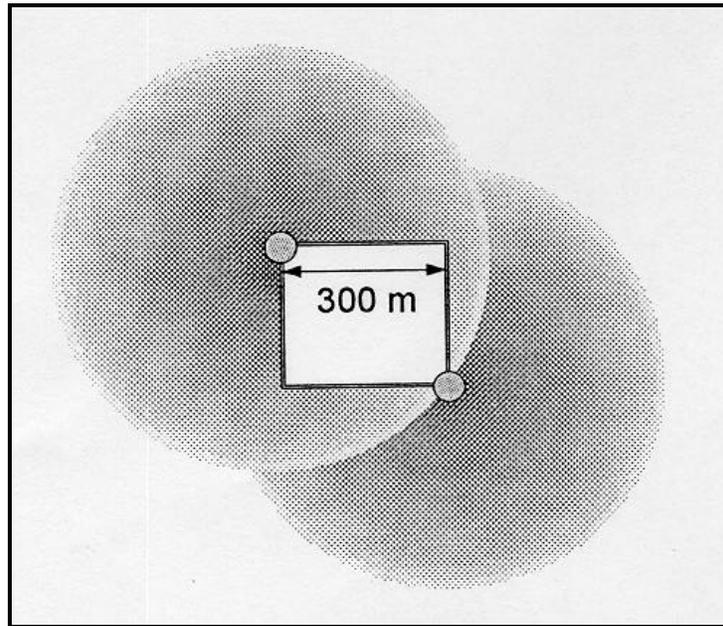
Figure 4. AES Deployed Around a Small Area

In figure 4, the 300 meter wide square represents a site and the circles represent detection ranges for individual AES RSM units.

Larger rectangular areas like runways that are up to two kilometers in length can be covered with six RSMs as figure 5 depicts.
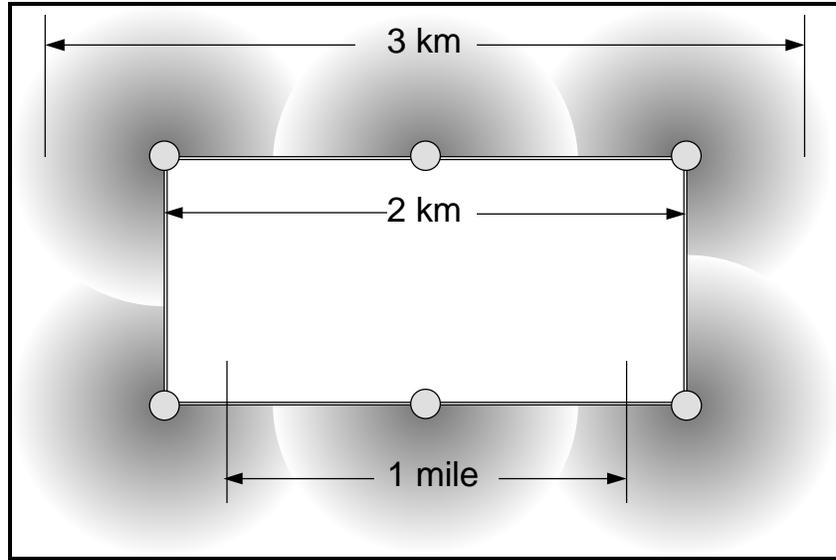
Figure 5. AES Deployed Around a Large Area

In figure 5, the rectangle represents the site and the circles represent detection ranges
for individual RSM units.

Also for larger areas where as many as 11 RSMs are available, a setup as in figure 6
might be appropriate where at least a two kilometer RSM radius detection zone is
provided around a protected facility. This scheme would be ideal for countering the
standoff threat discussed above where enemy forces could be as far as several kilometers
away from each end of an airfield's runway. If coverage is required over an even larger
area, and sufficient AES RSMs are not available, much less expensive TASS sensors
could be used to fill in gaps.

Figure 6. Expanded AES Coverage Around a Large Area With Uneven Terrain

In figure 6, the rectangle in the diagram's center represents the protected area and circles represent detection ranges for individual AES RSM units. One square equals 1000 feet.

Security police from the Air Staff, ESC/AVJ, and SNL must continue to work with Space Command and other major commands to explore all possible AES applications, whether the mission is base defense or space launch safety and security. This must be done today, in coordination with other service military police representatives, before AES

31

proceeds into advanced development stages. The AES figures depicted above should be part of a CONOPS, not a national laboratory or company brochure that "takes a best shot" at what engineers think might be required for force and resource protection.

Law Enforcement Operations

While people usually think of ATGSS in terms of the above discussed MOOTW and wartime environments, there are actually several law enforcement applications that should be explored. These applications will not only benefit the Department of Defense, but numerous other agencies such as the Federal Bureau of Investigations and the Department of Justice as well.

Consideration has been given to military technology in the law enforcement arena; however, the main focus has primarily been on advanced military command and control and intelligence systems (C4I). For example, law enforcement agencies can meet a number of high priority needs with components and sensors common in C4I systems, such as:

> Improved video and audio surveillance, body heat detection inside a building; creation of a two way dialog with criminals; quick identification of suspects by processing a verbal description or mug shot; real-time communication between officers and superiors; capability to tag and track vehicles; highway sensors that identify stolen cars; and radio transmitters attached to cars for timely deployment of cruisers.[28]

Not mentioned here, but being studied by Rome Laboratory in New York, is the use of real aperture radar, synthetic aperture radar, millimeter wave (MMW) radar, MMW radiometry and X-ray detection for wall penetration and surveillance applications.[29] As discussed above, the Air Force is also exploring MMW technology with the PMMWS that will improve TASS' tactical sensor capability by providing a sensor capable of

detecting through foliage. The PMMWS, although being an ATGSS, should be looked at for a law enforcement application as well to see through lightly constructed walls or similar barriers.

Other ATGSS offer numerous law enforcement applications. For example, sensors like TASS' active pulsed infrared or breakwire sensors that transmit alarm data by way of radio frequencies can have the battery or solar operated communication modules (CMs) or transmitters placed just about anywhere, such as on top of a bank or commissary. The CMs would relay the alarms received by sensors set up inside the facility to detect an attempted entry. Repeater antennas would allow alarms to be transmitted many kilometers away to patrols with hand-held or laptop annunciators who would receive alarms at the same time that a control center or law enforcement desk would. Having the patrols receive alarms would serve as a backup measure, allowing immediate response without delay. These applications would prove especially invaluable in remote locations where electricity may not be readily available for commonly used intrusion alarms. The cost to install tactical sensors might also be less expensive than alarms that rely on electricity.

Another ATGSS application can include the use of thermal imagers to monitor an area. While this is not a new idea since thermal imagers are being used to observe such areas as air base flightlines, much greater flexibility will be possible once a communications link like MMW is available instead of a hardwire connection. Without the hardwire connections, cameras could be set up anywhere and start sending images immediately.

Similar to tactical applications of ATGSS, law enforcement presents an arena wide open for ATGSS uses. It only takes further contemplation of these ideas today.

Notes

[1] DOD Directive 50002.2-M, *Defense Acquisition Management Documentation and Report*, February 1991, 2-1.

[2] Lt Col Mary Kay Hertog, "Nonlethal Weapons and Their Role in Military Police Missions: Future Fact or Fantasy," (Maxwell AFB, Ala: Air War College, 14 May 1996), 18.

[3] Gen (Ret) Wayne Downing, "The Downing Investigation Report," 30 August 1996, n.p.; on line, Internet, 30 December 1996, available from http://www.dtic.mil/defenselink/pubs/downing_rpt/unclf913.html.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] William J. Perry, Secretary of Defense, "Report to the President on the Protection of U.S. Forces Deployed Abroad," 15 September 1996, n.p. on line, Internet, 30 December 1996, available from http://www.dtic.mil/defenselink/pubs/downing_rpt/report_f.html.

[10] William Mathews, "The Blame Game: "We Will Remain Vulnerable to Terrorist Attacks," *Air Force Times*, 22 July 1996, n.p.; on-line, America Online, 1 January 1997.

[11] Lt John Flaherty, Air Force Electronic Security and Communications Center of Excellence, email, 31 October 1996.

[12] Hertog, *Nonlethal Weapons*, 22.

[13] Ibid., 1.

[14] Ibid., 8.

[15] David A. Shlapak and Alan Vick, *Check Six Begins on the Ground: Responding to the Evolving Ground Threat to U.S. Air Force Bases*, RAND Report MR-606-AF, (Santa Monica, Calif.: RAND Corporation, 1995).

[16] "Guarding Against Ground Attacks on U.S. Air Force Bases," *RAND Research Highlights*, undated, n.p.; on-line, Internet, 1 January 1997, available from http://www.rand-org/organization/paf/highlights.html.

[17] Shlapak and Vick, *Check Six Begins on the Ground*, 33.

[18] Ibid., 34.

[19] Air Force Electronic Security and Communications Center of Excellence, after action report, subject: Foal Eagle 93 Tactical Automated Security System Prototype Sensor Demonstration After Action Report, 7 January 1994, 8.

[20] Ibid.

[21] Lt Col James M. Shamess and Maj Michael F. Pasquin, security police staff, Headquarters U.S. Air Force, memorandum to the Air Force Chief of Security Police,

subject: Exercise Foal Eagle 94 and Orientation Visit to Other ABD Plans for Republic of Korea (ROK), 30 Oct 94 - 10 Nov 94, 22 November 1994, 3.

[22] Ibid.

[23] Ibid.

[24] Michael O'Stein, concept of employment, subject: Concept of Employment for Tactical Automated Security System (TASS), 29 December 1994, 1-9.

[25] Maj Michael F. Pasquin, transition plan, subject: Defense Nuclear Agency Physical Security Equipment (PSE) Transition Plan for the Advanced Exterior Sensor (AES), 22 May 1995, 3.

[26] Air Force Space Command, mission need statement, subject: Final Mission Need Statement (MNS) AFSPC 001-94 for Wide Area Security System (WASS) ACAT Level IV, 26 May 1995, 2.

[27] Headquarters Air Force security police, operational requirements document, subject: Operational Requirements Document (ORD) HQ USAF 006-93-I/II/III Priority Resource Security System (PRSS) ACAT Level III, 20 February 1996, 2-4.

[28] "Military Technologies Find New Law Enforcement Uses," *Signal*, November 1995, 55.

[29] Ibid., 57.

Chapter 5

Recommendations

The military *must* stay actively engaged in exploring as many options as possible for ATGSS. Several avenues exist to facilitate this endeavor. First, there is an immediate need to continue studying the Downing Report and other related reports concerning the Khobar Towers bombing to ensure security problems are closely and thoroughly examined. While the Downing Report uncovered problems with the inadequacy of security and the services improperly prioritizing and funding for security related technology, some outstanding security was provided by the Air Force and the Marines at other locations in Saudi Arabia.[1] All of this information needs looking at to see how similar environments can be secured better with ATGSS.

Second, regardless of the ATGSS—be it TASS, AES, or MSSMP—joint service system requirements must be explained in detailed CONOPS. Such documents will add to the minimum system performance requirements already outlined in MNSs and ORDs. It is only through such documentation that companies, national laboratories, and the service's PSE program offices that oversee ATGSS development, can stay appraised of the military's needs.

Third, besides ensuring the appropriate ATGSS documentation, services should take advantage of any single service, joint, or combined exercises like Foal Eagle or exercises

conducted at the joint regional training centers. These exercises bring forces together where ATGSS can be employed and aggressively tested in real-world scenarios. Before long, a plethora of information would be available greatly benefiting the future of force and resource protection.

Finally, in considering ATGSS, caution must be used not to slip into the past ways of doing business referred to in this paper. With AES, TASS, and other ATGSS, the national laboratory or contractor developing the system often writes their own version of a CONOPS. This offers an easy way out of doing the work that only the services should be doing in coordination with each other—properly considering ATGSS so that the job of providing security will ultimately be less difficult. Such consideration often comes only through long-term, faithful participation at ATGSS program reviews where employment concepts should be discussed years before a system is ever fielded.

Notes

[1] Gen (Ret) Wayne Downing, "The Downing Investigation Report," 30 August 1996, n.p.; on line, Internet, 30 December 1996, available from http:www.dtic.mil/defense link/pubs/downing_rpt/unclf913.html.

Chapter 6

Conclusion

Considering the multitude of technological advancements made in ATGSS in recent years, this paper contends that *more* thought should be given on how to employ these systems to avoid future Khobar Tower-type incidents. It is not enough that services have cooperated for years on basic research and development ideas for ATGSS. From the conclusions drawn in the Downing Report that point to a lack of "technology" in the field, to the lack of joint or even single-service CONOPS detailing ATGSS operational employment schemes, to recommendations from combined exercises like Foal Eagle that reveal no written procedures were available to help the military employ the new ATGSS, it is evident that ATGSS consideration is lacking. In the future, with the growing variety and complexity of military operations worldwide, it will only be through the thorough, comprehensive, and immediate consideration of ATGSS that force and resource protection will be performed much more effectively and efficiently.

The good news is that there is significant research and development recently completed or underway that will change ATGSS from being something based on decades-old technology that was at best barely adequate, to something that is an absolute necessity for effective military operations. Examples include systems like TASS—an ATGSS being fielded this year that is lightweight, robust, and can transmit alarms via 8000

selectable radio frequencies; to systems under development like AES that will scan, detect and classify intruders over large areas using two advanced sensors and video motion detection simultaneously.

As the military prepares for the multitude of missions and operations in next century, it will be the proper consideration of ATGSS today that will mean a much safer and secure future environment.

Glossary

AES	Advanced Exterior Sensor
ATGSS	attended tactical ground sensor systems
CONOPS	Concept of Operations
DSWA	Defense Special Weapons Agency (formerly Defense Nuclear Agency)
ESC/AVJ	Air Force Material Command's Electronic and Communications Center of Excellence
FITSS	Family of Integrated Tactical Security Systems
IREMBASS	Improved Remotely Monitored Battlefield Sensor System
MIDS	Miniature Intrusion Detection System
MMWDL	Millimeter Wave Data Link
MNS	Mission Need Statement
MSSMP	Multipurpose Security and Surveillance Mission Platform
MOOTW	military operations other than war
OPFOR	opposing force
ORD	Operational Requirements Document
PEWD II	Platoon Early Warning Device
PEWS	Platoon Early Warning System
PMMWS	Passive Millimeter Wave Sensor
PSE	Physical Security Equipment
PSEAG	Physical Security Equipment Action Group
RSM	Remote Sensor Monitor
SNL	Sandia National Laboratory
TASS	Tactical Automated Security System
UTGSS	unattended tactical ground sensor system
WASS	Wide-Area Security System

Bibliography

Air Force Space Command. Mission need statement. Subject: Final Mission Need Statement (MNS) AFSPC 001-94 for Wide Area Security System (WASS) ACAT Level IV, 26 May 1995.

Air Force Electronic Security and Communications Center of Excellence. After action report. Subject: Foal Eagle 93 Tactical Automated Security System Prototype Sensor Demonstration After Action Report, 7 January 1994.

Air Force Electronic Security and Communications Center of Excellence. Brochure. Subject: Tactical Automated Security System (TASS), 20 October 1994.

Army Physical Security Equipment Management Office. Tactical sensor comparison matrix, undated.

Army Communications and Electronics Command. Technical Information on the Platoon Early Warning System, 9 September 1996.

Army Material Systems Analysis Activity (AMSAA). Background paper. Subject: AMSAA Independent Evaluation for I-REMBASS Production Decision, 13 May 1992.

Army Infantry Center. Operational requirements document. Subject: Draft Operational Requirements Document for the Platoon Early Device II, 7 March 1996.

Army Physical Security Equipment Management Office. Information paper. Subject: Multipurpose Security and Surveillance Mission Platform, undated.

Army Training and Doctrine Command. Draft concept. Subject: Concept Statement (Final Draft) Family of Integrated Tactical Security Systems, undated.

Department of Defense Directive (DOD) 3224.3. *Physical Security Equipment (PSE): Assignment of Responsibility for research, Development, Testing, and Evaluation, Production, Procurement, Deployment, and Support*, 17 February 1989.

Department of Defense Directive (DOD) 5000.2-M. *Defense Acquisition Management Documentation and Report*, February 1991.

Downing, Gen (Ret) Wayne. "The Downing Investigation Report." 30 August 1996. n.p.; On line. Internet, 30 December 1996. Available from http://www.dtic.mil/defenselink/pubs/downing_rpt/unclf913.html.

"Guarding Against Ground Attacks on U.S. Air Force Bases." *RAND Research Highlights.* Undated. On-line. Internet, 1 January 1997. Available from http://www.rand-org/organization/paf/highlights.html.

Headquarters Air Force security police. Operational requirements document. Subject: Operational Requirements Document (ORD) HQ USAF 006-93-I/II/III Priority Resource Security System (PRSS) ACAT Level III, 20 February 1996.

Hertog, Mary Kay, "Nonlethal Weapons and Their Role in Military Police Missions: Future Fact or Fantasy." Maxwell AFB, Ala.: Air War College, 14 May 1996.

The Joint Staff. Background paper. Subject: Unattended MASINT Sensors, 10 September 1996.

Mathews, William, "The Blame Game: We Will Remain Vulnerable to Terrorist Attacks." *Air Force Times*, 22 July 1996. On-line. America Online, 1 January 1997.

Messner, Wayne K. Messner, "Air Force Systems Mold Defense Asset Security." *National Defense*, February 1995, 32-33.

Messner, Wayne K. "Organization is Key to Air Force Security System." *Access Control*, April 1995, 1-4.

Nicholas, Scott A. and Naylor, Brian R. Information paper. Subject: Reliable Motion Detection of Small Targets in Video with Low Signal-to-Clutter Ratios, undated.

O'Stein, M. Maj. Concept of employment. Subject: Concept of Employment for Tactical Automated Security System (TASS), 29 December 1994.

Pasquin, Michael F. Transition plan. Subject: Defense Nuclear Agency Physical Security Equipment (PSE) Exploratory Development to Advanced Development Transition Plan for Passive Millimeter Wave Sensor—Exterior (PMW-E), 22 May 1997.

Pasquin, Michael F. Transition plan. Subject: Defense Nuclear Agency Physical Security Equipment (PSE) Transition Plan for the Advanced Exterior Sensor (AES), 22 May 1995.

Pritchard, Daniel A. Information paper. Subject: System Overview and Applications of a Panoramic Imaging Perimeter Sensor, undated.

Qual-Tron Incorporated. Information paper. Subject: *Miniature Intrusion Detection System (MIDS),* undated.

Rogers, Robert L. Draft final technical report. Subject: Passive Millimeter Wave Sensor, 4 October 1996.

Sandia National Laboratory. Briefings slides. Subject: Advanced Exterior Sensor Program Review, 16 April 1996.

Sandia National Laboratory. Information paper. Subject: Advanced Exterior Sensor, May 1994.

Shamess, Lt Col J.M., and Pasquin, Maj M.F., Chief of Security Police staff, Headquarters Air Force. To the Air Force Chief of Security Police. Subject: Exercise Foal Eagle 94 and Orientation Visit to Other ABD Plans for Republic of Korea (ROK), 30 Oct 94 - 10 Nov 94, 22 November 1994.

Shapak, David A. *Check Six Begins on the Ground: Responding to the Evolving Ground Threat to U.S. Air Force Bases.* RAND Report MR-606-AF. Santa Monica, Calif.: RAND Corporation, 1995.

Perry, William J. Secretary of Defense; Gen John M. Shalikashvili, USA, Chairman of the Joint Chiefs of Staff; and Gen J.H. Binford Peay III, USA, Commander in Chief, U.S. Central Command. "Combating Terrorism in Saudi Arabia." Statements to the Senate Armed Services Committee, 9 July 1996, n.p.; On-line. Internet, 30 January 1996. Available from http://dtic.mil/defenselink/pubs/di96/di1159.html.

William J. Perry, Secretary of Defense. "Report to the President on the Protection of U.S. Forces Deployed Abroad," 15 September 1996, n.p. On line. Internet, 30 December 1996.Available   from http://www.dtic.mil/defenselink/pubs/downing_rpt/report_f.html.

"Military Technologies Find New Law Enforcement Uses," *Signal*, November 1995, 55-57.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air War College
Maxwell AFB, Al 36112